

# MULTIPLE HARMONIC SUMS AND WOLSTENHOLME'S THEOREM

JULIAN ROSEN

**ABSTRACT.** We give a family of congruences for the binomial coefficients  $\binom{kp-1}{p-1}$  in terms of multiple harmonic sums, a generalization of the harmonic numbers. Each congruence in this family (which depends on an additional parameter  $n$ ) involves a linear combination of  $n$  multiple harmonic sums, and holds mod  $p^{2n+3}$ . The coefficients in these congruences are integers depending on  $n$  and  $k$ , but independent of  $p$ . More generally, we construct a family of congruences  $\mathcal{F}_{2n,k}$  for  $\binom{kp-1}{p-1} \pmod{p^{2n+3}}$ , whose members contain a variable number of terms, and show that in this family there is a unique “optimized” congruence involving the fewest terms. The special case  $k = 2$  and  $n = 0$  recovers Wolstenholme's theorem  $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ , valid for all primes  $p \geq 5$ . We also characterize those triples  $(n, k, p)$  for which the optimized congruence holds modulo an extra power of  $p$ : they are precisely those with either  $p$  dividing the numerator of the Bernoulli number  $B_{p-2n-k}$ , or  $k \equiv 0, 1 \pmod{p}$ .

## 1. INTRODUCTION

In 1862 the Rev. J. Wolstenholme [25] noted the congruence that for all primes  $p \geq 5$ ,

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

This result is now called Wolstenholme's theorem. Later it was found that the related congruence on harmonic numbers  $H_n := \sum_{j=1}^n \frac{1}{j}$ , stating that for all primes  $p \geq 5$ ,

$$H_{p-1} \equiv 0 \pmod{p^2},$$

which was discovered earlier (by E. Waring [22] in 1782 and again by C. Babbage [2] in 1819), is in fact equivalent to Wolstenholme's result.

In the following 150 years, Wolstenholme's congruence has been generalized in many directions (see Meštrović [18] for a survey). This paper considers generalizations in two directions. The first direction treats a larger set of binomial coefficients, replacing  $2p-1$  with  $kp-1$ . In 1900 Glaisher [8] showed that for all integers  $k \geq 2$ ,

$$(1.1) \quad \binom{kp-1}{p-1} \equiv 1 \pmod{p^3}$$

holds for all  $p \geq 5$ . In 1999 Andrews [1] extended Glaisher's theorem to  $q$ -binomial coefficients.

The second direction obtains congruences modulo higher powers of  $p$ , by adding extra terms to the right hand side of Wolstenholme's congruence. In 2000 van

---

*Date:* January 31, 2013.

Hamme [10] proved a result implying that for all primes  $p \geq 7$ ,

$$(1.2) \quad \binom{2p-1}{p-1} \equiv 1 + 2p \sum_{j=1}^{p-1} \frac{1}{j} \pmod{p^5},$$

where  $H_n := \sum_{j=1}^n \frac{1}{j}$  are the harmonic numbers. Recently Meštrović [17] showed that for any prime  $p \geq 11$ ,

$$(1.3) \quad \binom{2p-1}{p-1} \equiv 1 - 2p \sum_{j=1}^{p-1} \frac{1}{j} + 4p^2 \sum_{\substack{1 \leq i < j \leq p-1}} \frac{1}{ij} \pmod{p^7}$$

This congruence involves the additional expression

$$\sum_{1 \leq i < j \leq p-1} \frac{1}{ij},$$

which is an example of a multiple harmonic sum, defined below.

The main result of this paper is a simultaneous generalization and unification of these results, giving congruences for  $\binom{kp-1}{p-1}$  to arbitrary powers of  $p$ , which involve multiple harmonic sums. Our basic method formulates and exploits the existence of families of linear relations between certain multiple harmonic sums. The coefficients in our congruences are given by certain polynomials  $b_{j,n}(T)$ , defined below.

**1.1. Main result.** A *composition* is a finite ordered list  $\{\lambda_1, \dots, \lambda_j\}$  of positive integers. For ease of notation, we will denote by  $\{\lambda_1, \dots, \lambda_j\}^a$  the composition

$$\underline{\lambda} = \{\underbrace{\lambda_1, \dots, \lambda_j}, \underbrace{\lambda_1, \dots, \lambda_j}, \dots, \underbrace{\lambda_1, \dots, \lambda_j}\}$$

consisting of  $a$  concatenated copies of  $\{\lambda_1, \dots, \lambda_j\}$ .

**Definition 1.1.** For a composition  $\underline{\lambda} = \{\lambda_1, \dots, \lambda_j\}$ , and a positive integer  $n$ , we define the *multiple harmonic sum*

$$H(\underline{\lambda}; n) := \sum_{n \geq i_1 > \dots > i_j \geq 1} \frac{1}{i_1^{\lambda_1} \cdot \dots \cdot i_j^{\lambda_j}}.$$

(By convention, if  $\underline{\lambda} = \{\lambda_1, \dots, \lambda_j\}$  and  $n < j$ , we set  $H(\underline{\lambda}; n) = 0$ )

For  $k$  an integer, it has long been known (see e.g. [16]) that the binomial coefficient  $\binom{kp-1}{p-1}$  can be written as a linear combination of ‘elementary symmetric’ multiple harmonic sums  $H(\{1\}^j; p-1)$ :

$$\binom{kp-1}{p-1} = \sum_{j=0}^{p-1} (k-1)^j p^j H(\{1\}^j; p-1)$$

For a fixed non-negative integer  $n$ , we may truncate this equation after the  $2n$ -th term and use estimates on the  $p$ -divisibility of the multiple harmonic sums  $H(\{1\}^j; p-1)$  to obtain the congruence

$$(1.4) \quad \binom{kp-1}{p-1} \equiv \sum_{j=0}^{2n} (k-1)^j p^j H(\{1\}^j; p-1) \pmod{p^{2n+3}}$$

which holds for all primes  $p \geq 2n+5$ .

In Section 2 we show that the generating function for the elementary symmetric multiple harmonic sums  $H(\{1\}^j; p-1)$  (with  $p$  fixed) satisfies a functional equation,

which we use to derive identities involving these sums. These identities can be used to cancel some of the terms appearing in (1.4). Our main result (like equation (1.4)) gives for each non-negative integer  $n$  a congruence for the binomial coefficient  $\binom{kp-1}{p-1}$  mod  $p^{2n+3}$ , involving multiple harmonic sums. However, our congruence involves only the first  $n$  elementary symmetric multiple harmonic sums (instead of the first  $2n$  such sums).

The coefficients in our congruences are given by polynomials in  $k$ . We make the following definition.

**Definition 1.2.** Let  $0 \leq j \leq n$  be integers. We define the *extremal polynomial*  $b_{j,n}(T) \in \mathbb{Q}[T]$  to be the unique polynomial of degree at most  $2n+1$  satisfying the following conditions:

- (C1)  $b_{j,n}(T) \equiv (T-1)^j \pmod{(T-1)^{n+1}}$
- (C2)  $b_{j,n}(T) \equiv (-1)^j T^j \pmod{T^{n+1}}$

A table of the extremal polynomials  $b_{j,n}(T)$  for  $0 \leq j \leq n \leq 3$  can be found in Section 1.2. Now we can state our main result:

**Theorem 1.3.** (Optimized Congruences) *Let  $n \geq 0$  be a fixed integer. The extremal polynomials  $b_{j,n}(T)$  ( $j = 0, 1, \dots, n$ ) have integer coefficients, and the following hold:*

- (1) *For every prime  $p \geq 2n+5$  and every integer  $k \geq 1$ :*

$$(1.5) \quad \binom{kp-1}{p-1} \equiv \sum_{j=1}^n b_{j,n}(k) p^j H(\{1\}^j; p-1) \pmod{p^{2n+3}}.$$

- (2) *If  $p = 2n+3$  is prime, then for every integer  $k \geq 1$ , the above congruence holds  $(\pmod{p^{2n+2}})$ .*
- (3) *For every prime  $3 \leq p \leq 2n+1$  and every integer  $k \geq 1$ , the above congruence is equality:*

$$\binom{kp-1}{p-1} = \sum_{j=1}^n b_{j,n}(k) p^j H(\{1\}^j; p-1).$$

Wolstenholme's congruence is the case  $n = 0, k = 2$  of Theorem 1.3. As another example, taking  $n = k = 3$  gives the congruence

$$\begin{aligned} \binom{3p-1}{p-1} \equiv & 1 + 402pH(\{1\}; p-1) - 396p^2H(\{1\}^2; p-1) \\ & + 216p^3H(\{1\}^3; p-1) \pmod{p^9}. \end{aligned}$$

Theorem 1.3 has four important features:

- (1) The coefficients  $b_{j,n}(k)$  appearing in the congruence (1.5) are independent of the prime  $p$ .
- (2) There are a large number of congruences for  $\binom{kp-1}{p-1}$  holding mod  $p^{2n+3}$ , which involve the multiple harmonic sums  $H(\{1\}^j; p-1)$  for  $1 \leq j \leq 2n$  (see Theorem 3.3). The congruences (1.5) are optimized among these in only containing the terms  $H(\{1\}^j; p-1)$  for  $1 \leq j \leq n$ .
- (3) The restriction of the theorem to exclude certain small primes, depending on  $n$ , is necessary. The congruences may fail to hold  $(\pmod{p^{2n+3}})$  for  $p = 2n+3$  (when  $2n+3$  is prime), and also fail to hold for  $p = 2$ .

(4) The extremal polynomials  $b_{j,n}(T)$  depend on  $n$ , and for fixed  $j$  their values at integers  $b_{j,n}(k)$ , which are the coefficients in the congruences, do *not* stabilize as  $n \rightarrow \infty$  (with the exception of  $b_{0,n}(k)$ ; see the tables in Section 1.2). However they do satisfy many interesting congruences as  $n$  varies, which we address in Section 6.

One may ask whether the coefficients  $b_{j,n}(k)$  appearing in the extremal congruences (1.5) are uniquely characterized by (1.5) holding for all sufficiently large primes  $p$ ; we conjecture this is the case, and discuss it in Section 1.3.

An *exceptional congruence* will be a triple  $(k, n, p)$  such that the corresponding congruence given in Theorem 1.3 holds modulo an extra power of  $p$ . We characterize exceptional congruences for primes  $p \geq 2n + 3$  as follows.

**Theorem 1.4.** (Exceptional Congruences) *Let  $n$  be a non-negative integer,  $p$  an odd prime. For all  $k \in \mathbb{Z}$ , we have the following:*

(i) *Suppose  $p \geq 2n + 5$ . The exceptional congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^n b_{j,n}(k) p^j H(\{1\}^j; p-1) \pmod{p^{2n+4}}$$

*holds if and only if either  $k \equiv 0, 1 \pmod{p}$  or  $p$  divides the numerator of the Bernoulli number  $B_{p-2n-3}$ .*

(ii) *Suppose  $p = 2n + 3$ . The exceptional congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^n b_{j,n}(k) p^j H(\{1\}^j; p-1) \pmod{p^{2n+3}}$$

*holds if and only if  $k \equiv 0, 1 \pmod{p}$ .*

We obtain Theorem 1.3 and Theorem 1.4 as special instances of a family  $\mathcal{F}_{N,k}$  of generalized Wolstenholme congruences, given in Theorem 3.3, and with the  $\mathcal{F}_{N,k}$  specified in Definition 3.4. The general congruence in the family  $\mathcal{F}_{N,k}$  (which will hold for all sufficiently large primes  $p$ ) is of the form

$$(1.6) \quad \binom{kp-1}{p-1} \equiv \sum_{j=0}^N b_j p^j H(\{1\}^j; p-1) \pmod{p^{N+1+\epsilon}}$$

where  $\epsilon \in \{1, 2\}$  is chosen so that  $\epsilon \equiv N \pmod{2}$ , and the coefficients  $b_j$  are rational numbers. Each congruence in this general family is derived from (1.4), using linear combinations of identities among multiple harmonic sums (these identities are stated as Theorem 2.2). The optimized congruence (1.5) is distinguished as the unique congruence in the family  $\mathcal{F}_{2n,k}$  satisfying  $b_{n+1} = b_{n+2} = \dots = b_{2n} = 0$ .

**1.2. The extremal polynomials  $b_{j,n}(T)$ .** In Section 6 we prove some interesting properties of the extremal polynomials  $b_{j,n}(T)$ . Here we present data on these polynomials for small  $j, n$  in Table 1 below.

Table 1 illustrates that  $b_{0,n}(T) = 1$  for all  $n$  (this will be established in Section 6). While the definition of  $b_{j,n}(T)$  given earlier shows that it has degree at most  $2n + 1$ , in fact its degree is at most  $2n$  (see Theorem 4.7).

We next consider the coefficients  $b_{j,n}(k)$  appearing in the extremal congruences given in Theorem 1.3. Values of the coefficients for  $k = 2$  and  $k = 3$  are given in Table 2 (resp. Table 3) below.

TABLE 1. Extremal Polynomials  $b_{j,n}(T)$ 

$n \setminus j$	0	1	2	3
0	1			
1	1	$T^2 - T$		
2	1	$-T^4 + 2T^3 - T$	$T^4 - 2T^3 + T^2$	
3	1	$2T^6 - 6T^5 + 5T^4 - T + 1$	$-2T^6 + 6T^5 - 5T^4 + T^2$	$T^6 - 3T^5 + 3T^4 - T^3$

TABLE 2. Values  $b_{j,n}(k)$  for  $k = 2$ 

$n \setminus j$	0	1	2	3	4	5
0	1					
1	1	2				
2	1	-2	4			
3	1	14	-12	8		
4	1	-66	68	-40	16	
5	1	382	-380	248	-112	32

Table 2 shows that  $b_{1,2}(2) = -2$ ,  $b_{2,2}(2) = 4$ , so that Theorem 1.3 reduces to Meštrović's result (1.3) in the case  $n = k = 2$ .

TABLE 3. Values  $b_{j,n}(k)$  for  $k = 3$ 

$n \setminus j$	0	1	2	3	4	5
0	1					
1	1	6				
2	1	-30	36			
3	1	402	-396	216		
4	1	-6078	6084	-3672	1296	
5	1	102786	-102780	66312	-29808	7776

Tables 2 and 3 illustrate that for  $j \geq 1$ , the coefficients  $b_{j,n}(k)$  which appear in the congruences (1.5) do not appear to stabilize as  $n \rightarrow \infty$  (holding  $j$  and  $k$  fixed).

**1.3. Uniqueness conjecture.** The statement of Theorem 1.3 raises an issue concerning whether the coefficients  $b_{j,n}(k)$  above are uniquely determined by the condition that the congruences (1.5) hold for all sufficiently large primes  $p$ . Theorem 4.1 asserts that there is a unique congruence of the form (1.5) in the general family  $\mathcal{F}_{N,k}$ . We believe that our family  $\mathcal{F}_{N,k}$  actually contains *all* congruences of the shape (1.6) which hold for all sufficiently large primes  $p$ , in which case the individual coefficients  $b_{j,n}(k)$  above would be uniquely determined by (1.5), but we do not establish this. We formulate this belief as the following conjecture.

**Conjecture 1.5.** (Uniqueness Conjecture)

Let  $n \geq 0$ ,  $k$  be integers,  $b_0, b_1, \dots, b_n \in \mathbb{Q}$  such that the congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^n b_j p^j H(\{1\}^j; p-1) \pmod{p^{2n+2}}$$

holds for all sufficiently large primes  $p$ . Then  $b_j = b_{j,n}(k)$  for  $j = 0, 1, \dots, n$ .

This conjecture might be difficult to resolve, in view of the following consequence.

**Proposition 1.6.** *In the special case  $n = k = 1$ , the Uniqueness Conjecture 1.5 implies that there are infinitely many primes  $p$  such that the numerator of the Bernoulli number  $B_{p-3}$  is not divisible by  $p$ .*

This property of the Bernoulli numbers is currently an open problem.

*Proof.* Take  $n = k = 1$ ,  $b_0 = b_1 = 1$ . These values do not agree with the values of the extremal coefficients  $b_{0,1}(1) = 1$ ,  $b_{1,1}(1) = 0$ , so the Uniqueness Conjecture states that there are infinitely many primes  $p \geq 7$  for which

$$1 = \binom{p-1}{p-1} \not\equiv 1 + pH(\{1\}; p-1) \pmod{p^4}.$$

That is, there are infinitely many primes  $p$  for which  $p^3 \nmid H(\{1\}; p-1)$ . Glaisher [7] showed that, for all primes  $p \geq 5$ ,

$$H(\{1\}; p-1) \equiv -\frac{B_{p-3}}{3}p^2 \pmod{p^3}.$$

The result now follows.  $\square$

In Section 3 we formulate a more general Strong Uniqueness Conjecture 3.6, which we show in Section 4 implies the Uniqueness Conjecture.

**1.4. Extensions of results.** Theorem 1.4 connects certain exceptional congruences with  $p$ -divisibility of the numerators of certain Bernoulli numbers. Recall that theorems of Herbrand and Ribet say that for odd  $i$  in the range  $3 \leq i \leq p-2$ ,  $p|B_{p-i}$  if and only if a particular piece of the class group of the cyclotomic field  $\mathbb{Q}(\zeta_p)$  has non-trivial  $p$ -part (see [23], Sec. 6.3 for a precise statement). This raises the possibility that our congruences may have an interpretation in terms of the arithmetic of cyclotomic fields. We do not currently know if that is the case, but in [19] we will show that there is a parallel family of congruences related to  $p$ -adic  $L$ -function values at positive integers, which involves the ‘power’ multiple harmonic sums  $H(\{j\}; p-1)$ . In [20] we systematically investigate the structure of identities among multiple harmonic numbers that underly such congruences.

**1.5. Related results.** The literature contains a vast collection of identities and congruences involving multiple harmonic sums and related sums, starting with work of Euler on harmonic numbers. Some of these involve binomial coefficient congruences (see Granville [9] for a survey). Our generalized congruences appear to have a structure not observed before, but for convenience we summarize some results from the literature for comparison.

A number of congruences are known for the elementary symmetric multiple harmonic sums  $H(\{1\}^r; n)$  considered in this paper. In 1900 Glaisher [7] proved that for all odd  $r \geq 5$  and all primes  $p \geq 7$ ,

$$S_r(p) := \frac{pr}{2}H(\{1\}^r; p-1) - H(\{1\}^{r-1}; p-1) \equiv 0 \pmod{p^4},$$

holds. In 1953 Carlitz [5] sharpened the congruence of Glaisher to show for all odd  $r \geq 5$  and prime  $p \geq 7$ ,

$$S_r(p) \equiv p^4 \frac{(p-r)(p-r-1)(p-r-2)}{24(p-r-3)(p-1)!} B_{p-3} \pmod{p^5},$$

giving a relation with Bernoulli numbers. Along similar lines, Tauraso [21] shows that for any prime  $p \geq 7$ ,

$$\begin{aligned} H(\{1\}; p-1) &\equiv -\frac{1}{2}pH(\{1\}^2; p-1) - \frac{1}{6}p^2H(\{1\}^3; p-1) \\ &\equiv p^2 \left( \frac{B_{2p-5}}{3p-5} - 3\frac{B_{2p-4}}{2p-4} + 3\frac{B_{p-3}}{p-3} \right) + p^4\frac{B_{p-5}}{p-5} \pmod{p^5} \end{aligned}$$

There are also many congruences known that involve power sum multiple harmonic sums

$$H(\{r\}, p-1) = \sum_{j=1}^{p-1} \frac{1}{j^r}.$$

Washington [24] provided a formula expressing these sums in terms of values of  $p$ -adic L-functions at positive integers. Congruences modulo  $p$  involving arbitrary multiple harmonic sums have been investigated by Hoffman [12].

Multiple harmonic sums appear in certain calculations in physics. Blümlein ([3] discussed applications of multiple harmonic sums to quantum field theory. He computed a family of algebraic relations between multiple harmonic sums  $H(\underline{\lambda}; n)$  which are independent of the upper limit of summation  $n$ . The Hopf algebra of quasi-symmetric functions has also been used by Hoffman to investigate both multiple harmonic sums [13] and multiple zeta values [11].

Kontsevich [15] considered the function

$$H_n(x) = \sum_{j=1}^n \frac{x^j}{j},$$

which is a ‘twisted’ version of a multiple harmonic sum. The expression  $H_n(x)$  may also be considered as a truncated version of the series  $-\log(1-x)$ . The corresponding sums for the dilogarithm  $\sum_{j=1}^n \frac{x^j}{j^2}$  were considered by Elbaz-Vincent and Gangl [6], who determine functional equations satisfied by such series. These values are truncated forms of multiple zeta values, which is of great current interest (see Zagier [26], Brown [4]).

## 2. REPRESENTING BINOMIAL COEFFICIENTS IN TERMS OF MULTIPLE HARMONIC SUMS

Our first object is to express binomial coefficients in terms of multiple harmonic sums. For  $n$  a positive integer, define the polynomial

$$f_n(T) = \binom{(n+1)(T+1)-1}{n} = \frac{1}{n!} \prod_{j=1}^n ((n+1)T+j)$$

It will be useful to rewrite  $f_n$  in the form

$$f_n(T) = \prod_{j=1}^n \left( 1 + \frac{n+1}{j} T \right)$$

Expanding the product above, we see that the coefficient of  $T^j$  is  $(n+1)^j$  times the  $j$ -th elementary symmetric function in  $1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}$ . In other words, we have

$$(2.1) \quad f_n(T) = \sum_{j=0}^n (n+1)^j H(\{1\}^j; n) T^j$$

By convention, we take  $H(\{1\}^j; n) = 0$  when  $j < 0$  or  $j > n$ . We also take  $H(\phi; n) = 1$ .

The polynomial  $f_n$  satisfies a functional equation relating  $T$  and  $-1 - T$ . We can compute

$$\begin{aligned} f_n(-1 - T) &= \frac{1}{n!} \prod_{j=1}^n ((n+1)(-1 - T) + j) \\ &= \frac{(-1)^n}{n!} \prod_{j=1}^n ((n+1)T + n + 1 - j) \\ &= \frac{(-1)^n}{n!} \prod_{i=1}^n ((n+1)T + i) \\ &= (-1)^n f_n(T) \end{aligned}$$

(In the third line we have made the substitution  $i = n + 1 - j$ ). We expand this functional equation using (2.1) to get

$$\begin{aligned} \sum_{j \geq 0} (n+1)^j H(\{1\}^j; n) T^j &= (-1)^n \sum_{j \geq 0} (n+1)^j H(\{1\}^j; n) (-1 - T)^j \\ &= \sum_{j \geq 0} (-1)^{n+j} (n+1)^j H(\{1\}^j; n) \sum_{0 \leq i \leq j} \binom{j}{i} T^i \\ &= \sum_{i \geq 0} \left( \sum_{j \geq i} \binom{j}{i} (-1)^{n+j} (n+1)^j H(\{1\}^j; n) \right) T^i \end{aligned}$$

This holds identically in  $T$ . Equating the coefficient of  $T^j$  on each side of the preceding equality and rearranging gives the following identity.

**Proposition 2.1.** *For all non-negative integers  $n, j$ , we have*

$$(2.2) \quad (n+1)^j H(\{1\}^j; n) + \sum_{i \geq j} (-1)^{n+i+1} \binom{i}{j} (n+1)^i H(\{1\}^i; n) = 0$$

The sum above is finite (terms corresponding to  $i > n$  vanish). We thus have a family of linear equations (indexed by  $j$ ) satisfied by the quantities  $(n+1)^i H(\{1\}^i; n)$ ,  $i = 0, 1, \dots, n$ .

From the above we obtain a general set of identities expressing binomial coefficients in terms of the  $H(\{1\}^j; n)$ .

**Proposition 2.2.** *Let  $n$  be a non-negative integer,  $k, c_0, c_1, \dots$  indeterminates, and define*

$$(2.3) \quad b_j := (k-1)^j + c_j + (-1)^{n+j+1} \sum_{i=0}^j \binom{j}{i} c_i.$$

*Then the equation*

$$(2.4) \quad \binom{k(n+1)-1}{n} = \sum_{j=0}^{\infty} b_j (n+1)^j H(\{1\}^j; n),$$

holds identically in the indeterminates  $k, c_0, c_1, \dots$ . Here the right side of (2.4) is a finite sum, since  $H(\{1\}^j; n) = 0$  for  $j > n$ .

*Proof.* To begin, we use Equation (2.1) to write

$$\begin{aligned} \binom{k(n+1)-1}{n} &= f_n(k-1) \\ &= \sum_{j \geq 0} (k-1)^j (n+1)^j H(\{1\}^j; n) \end{aligned}$$

Considering  $n$  fixed, we add to this equation a linear combination of equations (2.2) (where  $c_j$  is the coefficient of the equation indexed by  $j$ ) to obtain the general formula.  $\square$

**Remark 2.3.** By making suitable choices of the parameters  $c_i$  in Proposition 2.2, we can arrange to have  $b_j = 0$  for many  $j$ . Theorem 4.1 is obtained by optimizing this process. Special cases of the identities in this proposition were noted long ago. For example, Emma Lehmer ([16], p. 360) used the identity

$$\binom{p-1}{k} = (-1)^k \sum_{j=0}^k (-1)^j p^j H(\{1\}^j; k).$$

This particular identity is valid for all integers  $m$ , namely

$$\binom{m}{k} = (-1)^k \sum_{j=0}^k (-1)^j m^j H(\{1\}^j; k).$$

However most identities produced above hold only for restricted values of  $m$ , namely  $m = k(n+1) - 1$ , for fixed  $n$ .

### 3. CONGRUENCES FOR $\binom{kp-1}{p-1}$ MODULO POWERS OF $p$

To obtain congruences for  $\binom{kp-1}{p-1}$ , we will take  $k$  to be an integer and truncate the expansion of Proposition 2.2, with  $n = p-1$ ,  $p$  a prime. To establish a bound on the error due to truncation, we need to establish some congruence properties of multiple harmonic sums.

In the remainder of the paper, when  $p$  is understood to be a fixed prime, we sometimes abbreviate

$$H(\{1\}^j) := H(\{1\}^j; p-1).$$

**3.1. Congruence properties of multiple harmonic sums.** Zhao ([27], Theorem 1.6) gives the following congruence involving multiple harmonic sums  $H(\{1\}^j; p-1)$  and Bernoulli numbers:

**Proposition 3.1.** *Let  $p$  be a fixed odd prime, and  $j$  an integer with  $1 \leq j \leq p-3$ . Then we have*

$$H(\{1\}^j; p-1) \equiv \begin{cases} \frac{-B_{p-1-j}}{j+1} p \pmod{p^2} & \text{if } j \equiv 0 \pmod{2} \\ \left(\frac{(j+1)}{2(j+2)} B_{p-2-j}\right) p^2 \pmod{p^3} & \text{if } j \equiv 1 \pmod{2} \end{cases}$$

We provide additional congruence for  $H(\{1\}^j; p-1)$  for those  $j$  which are not covered by Proposition 3.1:

**Proposition 3.2.** *Let  $p$  be a fixed odd prime, and  $j$  a positive integer.*

- (i) If  $j = p - 2$  we have  $H(\{1\}^j; p - 1) \equiv \frac{1}{2}p \pmod{p^2}$ .
- (ii) If  $j = p - 1$ , we have  $H(\{1\}^j; p - 1) \equiv -1 \pmod{p}$ .
- (iii) If  $j \geq p$ , we have  $H(\{1\}^j; p - 1) = 0$ .

*Proof.* (i) We have

$$\begin{aligned} H(\{1\}^{p-2}) &= \sum_{i=1}^{p-1} \frac{1}{1 \cdots \hat{i} \cdots (p-1)} \\ &= \frac{1}{(p-1)!} \sum_{i=1}^{p-1} i \\ &= \frac{1}{(p-1)!} \frac{p(p-1)}{2} \\ &\equiv \frac{p}{2} \pmod{p^2} \end{aligned}$$

where in the last line, we have used Wilson's theorem, which states that  $(p-1)! \equiv -1 \pmod{p}$ .

(ii) We have

$$\begin{aligned} H(\{1\}^{p-1}) &= \frac{1}{(p-1)!} \\ &\equiv -1 \pmod{p} \end{aligned}$$

(iii) In this case the defining sum is empty. □

**3.2. A general family of congruences.** We can now obtain our general family of congruences for  $\binom{kp-1}{p-1}$ . The congruences are obtained from Proposition 2.2 by truncation. We take some care to express the error due to truncation in terms of Bernoulli numbers.

**Theorem 3.3** (General Wolstenholme-like Congruence). *Let  $k$  be an integer. Let  $c_0, c_1, \dots \in \mathbb{Q}$  be given, and take  $b_j \in \mathbb{Q}$  defined by*

$$(3.1) \quad b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i$$

*Fix an odd prime  $p$  which does not divide the denominator of any  $c_i$ , and let  $N$  be a non-negative integer. Define*

$$E_N := \binom{kp-1}{p-1} - \sum_{j=0}^N b_j p^j H(\{1\}^j; p - 1)$$

(i) If  $0 \leq N \leq p - 4$ , we have

$$E_N \equiv \frac{-B_{p-3-N}}{N+3} \left( \frac{N+2}{2} b_{N+1} + b_{N+2} \right) p^{N+3} \pmod{p^{N+4}}$$

when  $N$  is even, and

$$E_N \equiv \frac{-B_{p-2-N}}{N+2} b_{N+1} p^{N+2} \pmod{p^{N+3}}$$

when  $N$  is odd.

(ii) If  $N = p - 3$ , we have

$$E_N \equiv \left( \frac{b_{N+1}}{2} - b_{N+2} \right) p^{N+2} \pmod{p^{N+3}}$$

(iii) If  $N = p - 2$ , we have

$$E_N \equiv -b_{N+1} p^{N+1} \pmod{p^{N+2}}$$

(iv) If  $N \geq p - 1$ , we have

$$E_N = 0$$

In particular this implies that

$$(3.2) \quad \binom{kp-1}{p-1} \equiv \sum_{j=0}^N b_j p^j H(\{1\}^j) \left\{ \begin{array}{l} \text{mod } p^{N+3} \text{ if } N \leq p-4, \text{ } N \text{ even} \\ \text{mod } p^{N+2} \text{ if } N \leq p-4, \text{ } N \text{ odd} \\ \text{mod } p^{N+2} \text{ if } N = p-3 \\ \text{mod } p^{N+1} \text{ if } N = p-2 \\ \text{mod } 0 \text{ if } N \geq p-1 \end{array} \right.$$

(Congruence mod 0 means equality)

*Proof.* We apply Theorem 2.2 to obtain the equality

$$\binom{kp-1}{p-1} = \sum_{j=0}^{\infty} b_j p^j H(\{1\}^j).$$

Because  $n = p - 1$  is even, the values of  $b_i$  are independent of  $p$ . It follows that

$$E_N = \sum_{j=N+1}^{\infty} b_j p^j H(\{1\}^j)$$

We use Proposition 3.2, statement (iii) to eliminate the terms in the above some with  $j \geq p$ , giving

$$(3.3) \quad E_N = \sum_{N+1 \leq j \leq p-1} b_j p^j H(\{1\}^j)$$

The  $b_j$  are  $p$ -integral (because we assume the  $c_j$  to be  $p$ -integral). Propositions 3.1 and 3.2 also tell us that the expressions  $H(\{1\}^j)$  are  $p$ -integral. We now separate into cases.

**Case (i-a):** Suppose  $0 \leq N \leq p-5$  and  $N$  is even. Due to the integrality of  $b_j$  and  $H(\{1\}^j)$ , we have

$$\begin{aligned} E_N \equiv b_{N+1} p^{N+1} H(\{1\}^{N+1}) &+ b_{N+2} p^{N+2} H(\{1\}^{N+2}) \\ &+ b_{N+3} p^{N+3} H(\{1\}^{N+3}) \pmod{p^{N+4}} \end{aligned}$$

Proposition 3.1 tells us that  $H(\{1\}^{N+1}) \equiv \frac{-(N+2)}{2(N+3)} B_{p-3-N} p^2 \pmod{p^3}$  and  $H(\{1\}^{N+2}) \equiv \frac{-1}{N+3} p \pmod{p}$ . Also, Proposition 3.1 or Proposition 3.2 give that  $H(\{1\}^{N+3}) \equiv 0 \pmod{p}$ . Combining these give

$$E_N \equiv \frac{-B_{p-3-N}}{N+3} \left( \frac{N+2}{2} b_{N+1} + b_{N+2} \right) p^{N+3} \pmod{p^{N+4}},$$

as desired.

**Case (i-b):** Suppose  $0 \leq N \leq p-5$  and  $N$  is odd. Due to the integrality of  $b_j$  and  $H(\{1\}^j)$ , we have

$$E_N \equiv b_{N+1}p^{N+1}H(\{1\}^{N+1}) + b_{N+2}p^{N+2}H(\{1\}^{N+2}) \pmod{p^{N+3}}$$

Proposition 3.1 tells us that  $H(\{1\}^{N+1}) \equiv \frac{-1}{N+2}B_{p-2-N}p \pmod{p^2}$  and  $H(\{1\}^{N+2}) \equiv 0 \pmod{p^2}$ . This gives

$$E_N \equiv \frac{-B_{p-2-N}}{N+2}b_{N+1}p^{N+2} \pmod{p^{N+3}},$$

as desired.

**Case (i-c):** Suppose  $N = p-4$ . Due to the integrality of  $b_j$  and  $H(\{1\}^j)$ , we have

$$E_N \equiv b_{N+1}p^{N+1}H(\{1\}^{N+1}) + b_{N+2}p^{N+2}H(\{1\}^{N+2}) \pmod{p^{N+3}}$$

Proposition 3.1 tells us that  $H(\{1\}^{N+1}) \equiv \frac{-1}{N+2}B_{p-2-N}p \pmod{p^2}$ . Proposition 3.2 tells us that  $H(\{1\}^{N+2}) \equiv \frac{1}{2}p \pmod{p^2}$ . Combining these gives

$$E_N \equiv \frac{-B_{p-2-N}}{N+2}b_{N+1}p^{N+2} \pmod{p^{N+3}}$$

**Case (ii):** Suppose  $N = p-3$ . In this case (3.3) becomes

$$E_N = b_{N+1}p^{N+1}H(\{1\}^{p-2}) + b_{N+2}p^{N+2}H(\{1\}^{p-1})$$

Proposition 3.2 gives  $H(\{1\}^{p-2}) \equiv \frac{p}{2} \pmod{p^2}$  and  $H(\{1\}^{p-1}) \equiv -1 \pmod{p}$ , so

$$E_N \equiv \left( \frac{b_{N+1}}{2} - b_{N+2} \right) p^{N+2} \pmod{p^{N+3}}$$

**Case (iii):** Suppose  $N = p-2$ . In this case (3.3) becomes

$$E_N = b_{N+1}p^{N+1}H(\{1\}^{p-1})$$

Proposition 3.2 gives  $H(\{1\}^{p-1}) \equiv -1 \pmod{p}$ , so

$$E_N \equiv -b_{N+1}p^{N+1} \pmod{p^{N+2}}$$

**Case (iv):** Suppose  $N \geq p-1$ . Then (3.3) shows that  $E_N = 0$ .

□

**Definition 3.4.** We call the congruence (3.2) the *generalized Wolstenholme congruence* associated with the data

$$[k, (c_0, c_1, \dots), N],$$

and we will say that  $b_0, \dots, b_N$  are the *generalized Wolstenholme coefficients* associated with this data.

We let  $\mathcal{F}_{N,k}$  denote the family of all generalized Wolstenholme congruences above, where  $N, k$  are fixed and the other data varies.

**Remark 3.5.** For fixed  $k, N$ , the family  $\mathcal{F}_{N,k}$  has the structure of an affine linear space over  $\mathbb{Q}$  in the following way: if  $B = (b_0, \dots, b_N)$  and  $B' = (b'_0, \dots, b'_N)$  are the coefficients associated with the data  $[k, (c_0, c_1, \dots), N]$ ,  $[k, (c'_0, c'_1, \dots), N]$  respectively, and  $t \in \mathbb{Q}$ , then

$$tB + (1-t)B' = (tb_0 + (1-t)b'_0, \dots, tb_N + (1-t)b'_N),$$

where the numbers on right hand side are the generalized Wolstenholme coefficients associated with the data

$$[k, (tc_0 + (1-t)c'_0, tc_1 + (1-t)c'_1, \dots), N]$$

In the next section we will focus exclusively on the case where  $N = 2n$  is even. We will determine that the affine space of generalized Wolstenholme coefficients, for arbitrary  $k$  and  $N = 2n$ , has dimension  $n$ . The ‘optimized’ congruence will be uniquely determined among this  $n$  dimensional family.

Let  $N$  be a positive integer and set  $M = N + 3$  if  $N$  is even,  $M = N + 2$  if  $N$  is odd. It might be reasonable to expect that every congruence of the form

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^N b_j p^j H(\{1\}^j; p-1) \pmod{p^M}$$

that holds for all sufficiently large primes, actually comes from Theorem 3.3. We formulate this as the following conjecture:

**Conjecture 3.6.** (Strong Uniqueness Conjecture) *If  $k, m$  are integers with  $m \geq 0$ , and  $a_0, \dots, a_n \in \mathbb{Q}$  are such that*

$$\binom{kp-1}{p-1} \equiv a_0 + a_1 p H(\{1\}^1; p-1) + \dots + a_n p^n H(\{1\}^n; p-1) \pmod{p^m}$$

*holds for all but finitely many  $p$ , then this congruence arises from Theorem 3.3, in the following sense: there are constants  $c_0, c_1, \dots \in \mathbb{Q}$  such that, if  $b_0, b_1, \dots$  are defined by (3.1), then we have  $a_i = b_i$  for  $i = 0, 1, \dots, \psi(m)$ , where  $\psi(m) = m - 2$  if  $m$  is even and  $\psi(m) = m - 3$  if  $m$  is odd (here, we take  $a_i = 0$  for  $i > n$ ).*

Proposition 4.2 below will show that this conjecture implies the Uniqueness Conjecture 1.5.

Now we consider some special cases of Theorem 3.3. In what follows we will write  $(c_0, \dots, c_m)$  for the sequence  $(c_0, \dots, c_m, 0, 0, \dots)$ .

As one example, fix a positive integer  $k$  and take the data  $[k, ((k-1)^2), 2]$ . This gives  $(b_0, b_1, b_2, b_3, b_4) = (1, k(k-1), 0)$ , so we get the congruence

**Corollary 3.7.** *For all integers  $k$  and all primes  $p \neq 2, 5$ , we have*

$$\binom{kp-1}{p-1} \equiv 1 + k(k-1)p H(\{1\}; p-1) \pmod{p^5}$$

This is a generalization of van Hamme’s result (1.2).

Taking the data  $[2, (49, -18, 4), 6]$  gives

$(b_0, b_1, \dots, b_6) = (1, 14, -12, 8, 0, 0, 0)$ , so we get the identity

**Corollary 3.8.** *For all odd primes  $p$ , we have*

$$\begin{aligned} \binom{2p-1}{p-1} &\equiv 1 + 14p H(\{1\}^1; p-1) - 12p^2 H(\{1\}^2; p-1) \\ &\quad + 8p^3 H(\{1\}^3; p-1) \pmod{p^9} \end{aligned}$$

Corollaries 3.7 and 3.8 are special cases of Theorem 3.3, corresponding to  $n = 1$  and  $n = 3$ , respectively.

#### 4. OPTIMIZED WOLSTENHOLME CONGRUENCES

We now state a version of our main result (Theorem 1.3). We show that when  $N = 2n$  is even, it is always possible to choose the data  $(c_0, c_1, \dots)$  so that  $b_{n+1} = b_{n+2} = \dots = b_{2n} = 0$ . Moreover, this condition will uniquely determine the values of  $b_j$  for  $0 \leq j \leq n$ . We will derive this result using Theorem 3.3.

**Theorem 4.1** (Optimized Wolstenholme Congruences). *Let integers  $k, n$  be given, with  $n \geq 0$ , and set  $N = 2n$ . Then there exist unique values  $b_{j,n}(k) \in \mathbb{Q}$  ( $j = 0, 1, \dots, n$ ) with the following property:*

*There exist  $c_0, c_1, \dots \in \mathbb{Q}$  such that the generalized Wolstenholme coefficients  $b_0, b_1, \dots, b_N$  associated with the data  $[k, (c_0, c_1, \dots), N]$  satisfy  $b_j = b_{j,n}(k)$  for  $0 \leq j \leq n$ , and*

$$b_{n+1} = b_{n+2} = \dots = b_{2n} = 0$$

*Additionally, the  $c_j$  may be taken to be integers, so that the  $b_{j,n}(k)$  are necessarily integers.*

*In other words, for  $N = 2n$ , Theorem 3.3 produces a unique congruence of the form*

$$(4.1) \quad \binom{kp-1}{p-1} \equiv b_0 + b_1 p H(\{1\}^1; p-1) + \dots + b_n p^n H(\{1\}^n; p-1) \pmod{p^{2n+3}}$$

*with  $b_i \in \mathbb{Z}$ , which holds for all odd primes  $p \neq 2n+3$ .*

*In the case  $p = 2n+3$  we have*

$$(4.2) \quad \binom{kp-1}{p-1} \equiv b_0 + b_1 p H(\{1\}^1; p-1) + \dots + b_n p^n H(\{1\}^n; p-1) \pmod{p^{2n+2}}$$

*Additionally, for odd  $p \leq 2n+1$ , we have*

$$\binom{kp-1}{p-1} = b_0 + b_1 p H(\{1\}^1; p-1) + \dots + b_n p^n H(\{1\}^n; p-1)$$

We will defer the proof of this result, first showing that it gives an implication between the two uniqueness conjectures we have made.

**Proposition 4.2.** *The Strong Uniqueness Conjecture 3.6 implies the Uniqueness Conjecture 1.5.*

*Proof.* Let  $n \geq 0$ ,  $k$  be given, and suppose  $b_0, \dots, b_n \in \mathbb{Q}$  are taken such that the congruence

$$\binom{kp-1}{p-1} \equiv 1 + \sum_{j=1}^n b_j p^j H(\{1\}^j; p-1) \pmod{p^{2n+2}}$$

holds for all sufficiently large  $p$ . Suppose the Strong Uniqueness Conjecture 3.6 is true, and apply it with  $m = 2n+2$ , to find that there are  $c_0, c_1, \dots \in \mathbb{Q}$  such that

$$b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i$$

for  $j = 0, 1, \dots, n$ , and

$$(k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i = 0$$

for  $j = n+1, n+2, \dots, 2n$ . Now, the uniqueness statement of Theorem 4.1 above says that  $b_j = b_{j,n}(k)$  for  $j = 0, 1, \dots, n$ .  $\square$

For the proof of Theorem 4.1, we need some preliminary definitions and lemmas.

**Definition 4.3.** Fix integers  $N, k$ , with  $N \geq 0$ . Define  $V_{N,k} \subset \mathbb{Z}^{N+1}$  to be the set

$$V_{N,k} := \left\{ (b_0, \dots, b_N) : \exists c_0, c_1, \dots \in \mathbb{Z} \text{ s.t. } b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i \right\}$$

In other words  $V_{N,k}$  is the set of *generalized Wolstenholme coefficients* corresponding to integer data. We similarly define  $V_{N,k}^{\mathbb{Q}} \subset \mathbb{Q}^{N+1}$  to be

$$V_{N,k}^{\mathbb{Q}} := \left\{ (b_0, \dots, b_N) : \exists c_0, c_1, \dots \in \mathbb{Q} \text{ s.t. } b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i \right\},$$

the set of generalized Wolstenholme coefficients corresponding to rational data.

The inclusion  $V_{N,k} \hookrightarrow V_{N,k}^{\mathbb{Q}}$  induces an isomorphism

$$V_{N,k} \otimes \mathbb{Q} \cong V_{N,k}^{\mathbb{Q}}$$

of affine spaces over  $\mathbb{Q}$ .

We have that  $V_{N,k}$  is a coset of the subgroup

$$\hat{V}_N := \left\{ (b_0, \dots, b_N) : \exists c_0, c_1, \dots \in \mathbb{Z} \text{ s.t. } b_j = c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i \right\} \subseteq \mathbb{Z}^N$$

Note that  $\hat{V}_N$  is independent of  $k$ . We then have the following:

**Proposition 4.4.** For all integers  $N, k$ , with  $N \geq 0$ , we have  $V_{N,k} = V_{N,1-k}$ .

This is not surprising, as

$$\binom{kp-1}{p-1} = \binom{(1-k)p-1}{p-1}$$

holds for all odd primes  $p$  and all  $k$ .

*Proof.* As  $V_{N,k}$  and  $V_{N,1-k}$  are cosets of the same subgroup  $\hat{V}_N \leq \mathbb{Z}^{N+1}$ , equality will follow if we can show  $V_{N,k} \cap V_{N,1-k} \neq \emptyset$ .

Taking  $c_0 = c_1 = \dots = 0$ , we see  $(1, (-k), (-k)^2, \dots, (-k)^N) \in V_{N,1-k}$ . To see that this element is also in  $V_{N,k}$ , set  $c_j = -(k-1)^j$ . Then

$$\begin{aligned} b_j &= (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i \\ &= (k-1)^j - (k-1)^j + (-1)^j \sum_{i=0}^j \binom{j}{i} (k-1)^i \\ &= (-k)^j \end{aligned}$$

$\square$

**Lemma 4.5.** *For positive integers  $b, n$ , let  $M_{n,b}$  be the  $n \times n$  matrix*

$$M_{n,b} = \left( \binom{b+i}{j} \right)_{0 \leq i,j < n}$$

*Then  $\det M_{n,b} = 1$ .*

*Proof.* Define  $n \times n$  matrices  $L_n = \left( \binom{i}{j} \right)$ ,  $U_{n,b} = \left( \binom{b}{j-i} \right)$ .  $L_n$  is unipotent lower-triangular and  $U_{n,b}$  is unipotent upper-triangular, so both have determinant 1. We claim that  $M_{n,b} = L_n U_{n,b}$ , so that  $\det M_{n,b} = \det L_n \det U_{n,b} = 1$ . Looking at the entry in slot  $(i,j)$ , this equality reduces to the Vandermonde convolution identity

$$\binom{b+i}{j} = \sum_{k=0}^j \binom{i}{k} \binom{b}{j-k}$$

□

**Lemma 4.6.** *For all non-negative integers  $n$ ,  $\hat{V}_{2n}$  is a free  $\mathbb{Z}$ -module of rank  $n$ . Additionally, the map  $\pi : \hat{V}_{2n} \rightarrow \mathbb{Z}^n$  given by*

$$\pi(b_0, \dots, b_{2n}) = (b_{n+1}, \dots, b_{2n})$$

*is an isomorphism*

*Proof.* Here  $(b_0, \dots, b_{2n}) \in \hat{V}_{2n}$  is determined by the values of  $c_j$  for  $0 \leq j \leq 2n$ . We therefore have a surjective map  $\varphi_n : \mathbb{Z}^{2n+1} \rightarrow \hat{V}_{2n} \leq \mathbb{Z}^{2n+1}$ , taking  $(c_0, \dots, c_{2n})$  to  $(a_0, \dots, a_{2n})$  with

$$a_j = c_j + (-1)^{j+1} \sum_{i=0}^j \binom{j}{i} c_i$$

In other words the matrix representing  $\varphi_n$  (with respect to the standard basis on  $\mathbb{Z}^{2n+1}$ ) is given by

$$A_n := \left( \delta_{i,j} + (-1)^{j+1} \binom{j}{i} \right)_{0 \leq i,j \leq 2n}$$

If we identify row vectors of length  $2n+1$  with the set of polynomials of degree at most  $2n$  via the identification  $(a_0, \dots, a_{2n}) \leftrightarrow a_0 + a_1 T + \dots + a_{2n} T^{2n}$ , then the  $j$ -th row of  $A_n$  is identified with the polynomial

$$T^j - (-1 - T)^j$$

This means that the row span of  $A_n$  is contained in the set of polynomials  $f(T)$  satisfying  $f(T) = -f(-1 - T)$ . Such polynomials can be written as  $\mathbb{Q}$ -linear combinations of  $T + \frac{1}{2}, (T + \frac{1}{2})^2, \dots, (T + \frac{1}{2})^{2n-1}$ . It follows that  $\text{rank}(\hat{V}_{2n}) = \text{rank}(A_n) \leq n$ .

Next let  $i : \mathbb{Z}^n \rightarrow \mathbb{Z}^{2n+1}$ ,  $(x_0, \dots, x_{n-1}) \mapsto (x_0, \dots, x_{n-1}, 0, 0, \dots, 0)$ . We have  $\pi \circ \varphi_n \circ i(x_0, \dots, x_{n-1}) = (y_1, \dots, y_n)$ , where

$$y_j = (-1)^{n+j} \sum_{i=0}^{n-1} \binom{n+1+j}{i} x_i$$

By Lemma 4.5, this map is bijective. It follows that  $\pi$  is surjective. Since  $\text{rank}(\hat{V}_{2n}) \leq n = \text{rank}(\mathbb{Z}^n)$ , we must have that  $\text{rank}(\hat{V}_{2n}) = n$ , and  $\pi$  is bijective. □

*Proof of Theorem 4.1.* We need to show that there is a unique element of the form

$$(b_0, \dots, b_n, 0, 0, \dots, 0) \in V_{2n,k}^{\mathbb{Q}},$$

and that  $b_0, \dots, b_n \in \mathbb{Z}$ . It suffices to show there is a unique element of this form in  $V_{2n,k}$ . Because  $V_{2n,k} = (1, (k-1), \dots, (k-1)^{2n}) + \hat{V}_{2n}$ , this is equivalent to showing there is a unique element of the form

$$\underline{a} = (a_0, \dots, a_n, -(k-1)^{n+1}, \dots, -(k-1)^{2n}) \in \hat{V}_{2n}$$

This is the same as finding an  $\underline{a} \in \hat{V}_{2n}$  with  $\pi(\underline{a}) = (-(k-1)^{n+1}, \dots, -(k-1)^{2n})$ . Such an  $\underline{a}$  exists and is unique by Lemma 4.6.

That the values  $b_{j,n}(k)$  agree with a polynomial in  $k$  will follow from Corollary 4.7 below.  $\square$

We summarize the recipe for constructing the coefficients  $b_{j,n}(k)$  given in Theorem 4.1. It will follow that these coefficients are interpolated by a polynomial  $b_{j,n}(T)$ .

**Theorem 4.7.** *For fixed integers  $0 \leq j \leq n$ , the coefficients  $b_{j,n}(k)$  given in Theorem 4.1 are values of a polynomial  $b_{j,n}(T)$  at  $T = k$ , which is of degree at most  $2n$ . This polynomial can be computed explicitly as follows.*

Let  $M_n$  be the  $n \times n$  matrix

$$M_n = \left[ (-1)^{n+i} \binom{n+1+i}{j} \right]_{0 \leq i, j \leq n-1}$$

Let  $D_n$  be the  $(n+1) \times n$  matrix

$$D_n = \left[ (-1)^{i+1} \binom{i}{j} + \delta_{i,j} \right]_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n-1}}$$

where  $\delta_{i,j}$  is the Kronecker delta. Then  $M_n$  is invertible over the integers, and we have the matrix equation

$$(4.3) \quad \begin{pmatrix} b_{0,n}(k) \\ b_{1,n}(k) \\ \vdots \\ b_{n,n}(k) \end{pmatrix} = \begin{pmatrix} (k-1)^0 \\ (k-1)^1 \\ \vdots \\ (k-1)^n \end{pmatrix} - D_n \cdot M_n^{-1} \cdot \begin{pmatrix} (k-1)^{n+1} \\ (k-1)^{n+2} \\ \vdots \\ (k-1)^{2n} \end{pmatrix}$$

In particular this shows that  $b_{j,n}(k)$  is given by a polynomial in  $k$ , of degree at most  $2n$ , having integer coefficients.

*Proof.* The formula (4.3) follows from the proof of Theorem 4.1. This formula implies that  $b_{j,k}(k)$  is given by a polynomial in  $k$ , of degree at most  $2n$ , having integer coefficients.  $\square$

**Definition 4.8.** For integers  $j, n, k$ , with  $j, n \geq 0$ , we let  $b_{j,n}(k)$  denote the coefficients arising from Theorem 4.1. We call these *extremal coefficients*. We also denote by  $b_{j,n}(T)$  the polynomial giving these coefficients, and call these *extremal polynomials*. By convention, we take  $b_{j,n}(T) = 0$  for  $n+1 \leq j \leq 2n$ , and we say that  $b_{j,n}(T)$  is not defined for  $j \geq 2n+1$ .

Theorem 4.7 provides a recipe for computing the extremal coefficients in terms of matrices involving binomial coefficients. In this sense they are like the Bernoulli numbers, which can be computed by a similar expression.

Proposition 4.4 says that  $V_{2n,k} = V_{2n,1-k}$ . We may therefore make the substitution  $k \leftrightarrow 1 - k$  in Theorem 4.7 to get the following:

**Corollary 4.9.** *Let  $k, n$  be given, and set  $N = 2n$ . Let  $D_n, M_n$  be as in the statement of Theorem 4.7. Then*

$$(4.4) \quad \begin{pmatrix} b_0(k, n) \\ b_1(k, n) \\ \vdots \\ b_n(k, n) \end{pmatrix} = \begin{pmatrix} (-k)^0 \\ (-k)^1 \\ \vdots \\ (-k)^n \end{pmatrix} - D_n \cdot M_n^{-1} \cdot \begin{pmatrix} (-k)^{n+1} \\ (-k)^{n+2} \\ \vdots \\ (-k)^{2n} \end{pmatrix}$$

We can combine Theorem 4.7 and Corollary 4.9 to obtain the following characterization of the extremal polynomials  $b_{j,n}(T)$ :

**Proposition 4.10.** *Fix integers  $j, n$ , with  $j \leq 2n$ . The extremal polynomial  $b_{j,n}(T) \in \mathbb{Z}[T]$  is the unique polynomial of degree at most  $2n$  satisfying the following conditions:*

- (i)  $b_{j,n}(T) \equiv (T-1)^j \pmod{(T-1)^{n+1}}$
- (ii)  $b_{j,n}(T) \equiv (-T)^j \pmod{T^{n+1}}$

*Proof.* For  $n+1 \leq j \leq 2n$ ,  $b_{j,n}(T) = 0$ , and the result can be seen directly. For  $j \leq n$ , Corollary 4.7 shows that  $\deg(b_{j,n}(T)) \leq 2n$ , and that  $b_{j,n}(T)$  is equal to  $(T-1)^j$  plus a  $\mathbb{Z}$ -linear combination of  $(T-1)^{n+1}, \dots, (T-1)^{2n}$ . This shows that (i), (ii) are satisfied. Condition (iii) similarly follows from Corollary 4.9.

For uniqueness, the Chinese remainder theorem says that conditions (ii), (iii) determine the residue class of  $b_{j,n}(T)$  modulo  $T^{n+1}(T-1)^{n+1}$ . There will, a fortiori, be only one polynomial with rational coefficients and degree at most  $2n+1$  in this residue class. Our computations have shows that this polynomial in fact has integer coefficients and degree at most  $2n$ .  $\square$

Theorem 1.3, stated in the introduction, now follows from the combination of Theorem 4.1, Theorem 4.7, and Proposition 4.10.

## 5. EXCEPTIONAL CONGRUENCES AND BERNOULLI NUMBERS

We now investigate the situations under which the congruences (4.1), (4.2) hold modulo some larger power of  $p$  than given by Theorem 4.1. We term these *exceptional congruences*. In the case of Wolstenholme's theorem, we have that the exceptional congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$$

holds if and only if  $p$  divides the numerator of the Bernoulli number  $B_{p-3}$  (this follows from the results of van Hamme [10] and Glaisher [7]). We establish a similar result, which shows that the congruences (4.1), (4.2) hold modulo an extra power of  $p$  if and only if either  $p|B_{p-2n-3}$ , or  $p|k(k-1)$ .

Let non-negative integers  $n, k$  be given, and choose  $c_0, c_1, \dots \in \mathbb{Z}$  so that the generalized Wolstenholme congruence associated with the data  $[k, (c_0, c_1, \dots), 2n]$  is the optimal one, given by Theorem 4.1 (the  $c_i$  are not uniquely determined by this condition). Let  $b_0, b_1, \dots, b_{2n+2}$  be given by (3.1), so that  $b_j = b_{j,n}(k)$  for  $j = 0, 1, \dots, n$ , and  $b_j = 0$  for  $j = n+1, n+2, \dots, 2n$ . The values of  $b_{2n+1}$  and  $b_{2n+3}$  will depend on the choice of the  $c_i$ .

**Proposition 5.1.** *Define*

$$C_n(k) := (n+1)b_{2n+1} + b_{2n+2}$$

*Then, independent of the choice of  $c_i$  giving the optimal congruence, we have  $C_n(k) = k^{n+1}(k-1)^{n+1}$ .*

*Proof.* First we show that the value of  $C_n(k)$  depends only on  $n$  and  $k$ , but not the choice of  $c_i$ . Let  $p : V_{2n+2,k} \rightarrow V_{2n,k}$ ,  $(b_0, \dots, b_{2n+2}) \mapsto (b_0, \dots, b_{2n})$  be the projection map (where  $V_{\cdot,k}$  is given by Definition 4.3). From the construction of the spaces  $V_{2n+1,k}$ ,  $V_{2n,k}$ ,  $p$  is surjective. Lemma 4.6 says that  $\text{rank}(V_{2n+2,k}) = n+1$ ,  $\text{rank}(V_{2n,k}) = n$ . It follows that  $U := p^{-1}(b_0, b_1, \dots, b_n, 0, \dots, 0)$  is a  $\mathbb{Z}$  torsor. Therefore, if we can exhibit  $(b'_0, \dots, b'_{2n+2}) \neq (b_0, \dots, b_{2n+3}) \in U$  such that  $(n+1)b'_{2n+1} + b'_{2n+2} = (n+1)b_{2n+1} + b_{2n+2}$ , we will be done.

If we take  $c'_i = c_i$  for  $i \neq 2n+1$ , and  $c'_{2n+1} = c_{2n+1} + 1$ , we will have that  $b'_i = b_i$  for  $i \leq 2n$ ,  $b'_{2n+1} = b_{2n+1} + \binom{2n+1}{1}$ , and  $b'_{2n+2} = b_{2n+2} - \binom{2n+2}{2}$ . It follows directly that  $(n+1)b'_{2n+1} + b'_{2n+2} = (n+1)b_{2n+1} + b_{2n+2}$ .

Next we show that  $C_n(k)$  agrees with a polynomial in  $k$ . Using the same process as in Corollary 4.7, we may solve for the data  $c_0, \dots, c_{2n}$  to give the extremal congruence. We will use this data (with  $c_i = 0$  for  $i \geq 2n+1$ ). We can then compute  $b_{2n+1}$ ,  $b_{2n+2}$  in the following way:

Let  $M_n$  be the  $n \times n$  matrix

$$M_n = \left[ (-1)^{n+i} \binom{n+1+i}{j} \right]_{0 \leq i, j \leq n-1}$$

Let  $A_n$  be the  $2 \times n$  matrix

$$A_n = \left[ (-1)^{i+1} \binom{i}{j} + \delta_{i,j} \right]_{\substack{2n+1 \leq i \leq 2n+2 \\ 0 \leq j \leq n-1}}$$

where  $\delta_{i,j}$  is the Kronecker delta. Then  $M_n$  is invertible over the integers, and we have the matrix equation

$$(5.1) \quad \begin{pmatrix} b_{2n+1} \\ b_{2n+2} \end{pmatrix} = \begin{pmatrix} (k-1)^{2n+1} \\ (k-1)^{2n+2} \end{pmatrix} - A_n \cdot M_n^{-1} \cdot \begin{pmatrix} (k-1)^{n+1} \\ (k-1)^{n+2} \\ \vdots \\ (k-1)^{2n} \end{pmatrix}$$

This shows that  $b_{2n+1}$ ,  $b_{2n+2}$  are polynomials in  $k$ . Moreover,  $b_{2n+1}$  is equal to  $(k-1)^{2n+1}$  plus a  $\mathbb{Z}$ -linear combination of  $(k-1)^{n+1}, \dots, (k-1)^{2n}$ , so that  $b_{2n+1}$  is monic in  $k$ , of degree  $2n+1$ , and  $(k-1)^{n+1} | b_{2n+1}$ . Similarly,  $b_{2n+2}$  is monic of degree  $2n+2$ , and  $(k-1)^{n+1} | b_{2n+2}$ . It follows that  $C_n(k) = (n+1)b_{2n+1} + b_{2n+2}$  is monic of degree  $2n+2$ , with  $(k-1)^{2n+1} | C_n(k)$ . Moreover,  $C_n(k)$  is determined by the set  $V_{2n+2,k}$ , and Lemma 4.4 says that  $V_{2n+2,k} = V_{2n+2,1-k}$ . We may therefore make the substitution  $k \leftrightarrow 1-k$  to get the  $k^{n+1} | C_n(k)$ . By the Chinese remainder theorem,  $k^{n+1}(k-1)^{n+1} | C_n(k)$ . The only monic polynomial of degree  $2n+2$  which is divisible by  $k^{n+1}(k-1)^{n+1}$  is  $k^{n+1}(k-1)^{n+1}$ , so we conclude  $C_n(k) = k^{n+1}(k-1)^{n+1}$ .  $\square$

We now consider the possibility of extra powers of  $p$  in the congruences (4.1), (4.2). For all integers  $k, n$  with  $n \geq 0$ , and all odd primes  $p$ , define

$$E(k, n, p) := \binom{kp-1}{p-1} - \sum_{j=0}^n b_{j,n}(k) p^j H(\{1\}^j)$$

**Proposition 5.2.** *Suppose  $p \geq 2n + 5$ . Then*

$$E(k, n, p) \equiv \frac{-B_{p-3-2n}}{2n+3} k^{n+1} (k-1)^{n+1} p^{2n+3} \pmod{p^{2n+4}}$$

*Proof.* By Theorem 3.3, we have

$$E(k, n, p) \equiv b_{2n+1} p^{2n+1} H(\{1\}^{2n+1}) + b_{2n+2} p^{2n+2} H(\{1\}^{2n+2}) \pmod{p^{2n+4}}$$

Using Proposition 3.1, we can write

$$\begin{aligned} E(k, n, p) &\equiv -b_{2n+1} p^{2n+3} \frac{2n+2}{2(2n+3)} B_{p-3-2n} - b_{2n+2} p^{2n+3} \frac{B_{p-3-2n}}{2n+3} \\ &\equiv \frac{-B_{p-3-2n}}{n+3} ((n+1)b_{2n+1} - b_{2n+2}) \\ &\equiv \frac{-B_{p-3-2n}}{n+3} k^{n+1} (k-1)^{n+1} \pmod{p^{2n+4}} \end{aligned}$$

□

**Proposition 5.3.** *Suppose  $p = 2n + 3$ . Then*

$$E(k, n, p) \equiv -k^{n+1} (k-1)^{n+1} p^{2n+2} \pmod{p^{2n+3}}$$

*Proof.* By Theorem 3.3, we have

$$E(k, n, p) = b_{2n+1} p^{2n+1} H(\{1\}^{2n+1}) + b_{2n+2} p^{2n+2} H(\{1\}^{2n+2})$$

Using Proposition 3.1, we can write

$$\begin{aligned} E(k, n, p) &\equiv \frac{b_{2n+1}}{2} p^{2n+2} - b_{2n+2} p^{2n+2} \\ &\equiv \left( -\frac{(p-1)b_{2n+1}}{2} - b_{2n+1} \right) p^{2n+2} \\ &\equiv -((n+1)b_{2n+1} + b_{2n+2}) \\ &\equiv -k^{n+1} (k-1)^{n+1} p^{2n+2} \pmod{p^{2n+3}} \end{aligned}$$

□

We can now state the precise conditions under which the congruences (4.1), (4.2) hold modulo a larger power of  $p$  than is given by Theorem 4.1. The following Theorem is an immediate consequence of the preceding two propositions:

**Theorem 5.4.** *Let  $n \geq 0$ ,  $k$  be integers,  $p$  an odd prime, and  $b_{j,n}(T)$  the extremal polynomials (characterized by Proposition 4.10).*

(i) *Suppose  $p \geq 2n + 5$ . The congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^n b_{j,n}(k) p^j H(\{1\}^j; p-1) \pmod{p^{2n+4}}$$

*holds if and only if either  $p|B_{p-3-2n}$  or  $k \equiv 0, 1 \pmod{p}$ .*

(ii) *Suppose  $p = 2n + 3$ . The congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^n b_{j,n}(k) p^j H(\{1\}^j; p-1) \pmod{p^{2n+3}}$$

*holds if and only if  $k \equiv 0, 1 \pmod{p}$ .*

## 6. PROPERTIES OF THE EXTREMAL POLYNOMIALS

The extremal polynomials  $b_{j,n}(T)$  satisfy many arithmetic and congruence relations.

**Proposition 6.1.** *The extremal polynomials  $b_{j,n}(T)$  satisfy the following properties:*

- (i) *For all non-negative integers  $n$ ,  $b_{0,n}(T) = 1$*
- (ii) *For all non-negative integers  $n$ ,  $b_{n,n}(T) = T^n(T-1)^n$*
- (iii) *For all non-negative integers  $j \leq 2n$ ,  $T^j(T-1)^j$  divides  $b_{j,n}(T)$ .*

*Proof.* (i) and (ii) follow by checking that the given polynomial satisfies the conditions of Proposition 4.10. (iii) also follows immediately from Proposition 4.10.  $\square$

For fixed  $j$ , the polynomials  $b_{j,n}(T)$  depend on  $n$ . One exception to this is that  $b_{0,n}(T) = 1$  for all non-negative integers  $n$ . Examining the table in Section 1.2, we see that  $b_{1,n}(T)$  does indeed depend on  $n$ . However,  $b_{1,n}(T) + b_{2,n}(T) = T^2 - T$  for all  $n$ .

This is the first in a family of equations giving linear combinations of the extremal polynomials  $b_{j,n}(T)$  ( $j$  varying) which are independent of  $n$ .

**Proposition 6.2.** *Let  $m$  be a non-negative integer. Suppose we are given  $f(T) = \sum_{j=0}^m a_j T^j \in \mathbb{Q}[T]$  satisfying  $f(T) = f(-1-T)$ . Then, for all non-negative integers  $n$  with  $2n \geq m$ , we have*

$$\sum_{j=0}^m a_j b_{j,n}(T) = f(T-1)$$

*Proof.* Define

$$g(T) = \sum_{j=0}^m a_j b_{j,n}(T)$$

By Proposition 4.10, we have  $b_{j,n}(T) \equiv (T-1)^j \pmod{(T-1)^{n+1}}$ , so that

$$\begin{aligned} g(T) &\equiv \sum_{j=0}^m a_j (T-1)^j \\ &\equiv f(T-1) \pmod{(T-1)^{n+1}} \end{aligned}$$

Similarly, by Proposition 4.10, we have  $b_{j,n}(T) \equiv (-T)^j \pmod{T^{n+1}}$ , so that

$$\begin{aligned} g(T) &\equiv \sum_{j=0}^m a_j (-T)^j \\ &\equiv f(-T) \\ &\equiv f(T-1) \pmod{(T-1)^{n+1}} \end{aligned}$$

By the Chinese remainder theorem, it follows that

$g(T) \equiv f(T-1) \pmod{T^{n+1}(T-1)^{n+1}}$ . Now, we just note that  $g(T)$  and  $f(T-1)$  have degree at most  $2n+1$ , so they must be equal.  $\square$

**Acknowledgments.** I thank J. Lagarias for pointing out this problem, and for editorial comments and references. I also thank E. H. Brooks for introducing the author to Wolstenholme's theorem, and for helpful comments. This work was supported in part by NSF grants DMS-0943832 and DMS-1101373.

## REFERENCES

1. G. E. Andrews,  $q$ -analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher, *Discrete Math.* **204** (1999), No. 1–3, 15–25.
2. C. Babbage, Demonstration of a theorem relating to prime numbers, *The Edinburgh Philosophical Journal* **1** (1819), 46–49.
3. J. Blümlein, Algebraic relations between harmonic sums and associated quantities, *Computer Physics Communications* No. 159 (2004), pp. 19–54
4. F. Brown, Mixed Tate motives over  $\mathbb{Z}$ , *Annals of Math.* **175** (2012), No. 2, 949–976.
5. L. Carlitz, Note on a theorem of Glaisher, *J. London Math. Soc.* **28** (1953), 245–246.
6. P. Elbaz-Vincent and H. Gangl, On poly(ana) logs I. *Compositio Math.* **130** (2002), no. 2, 161–210.
7. J. W. L. Glaisher, Congruences relating to the sums of products of the first  $n$  numbers and to other sums and products, *Quart. J. Math.* **31** (1899), 2–35.
8. J. W. L. Glaisher, On the residues of the sums of the inverse powers of numbers in arithmetical progression, *Quart. J. Math.* **32** (1900), 271–288.
9. A. Granville, Arithmetic properties of binomial coefficients I.: Binomial coefficients modulo prime powers, In: *Organic Mathematics, Burnaby, BC, 1995*, CMS Conference Proc. vol. 20, Amer. Math. Soc.: Providence 1997, pp. 253–276.
10. L. van Hamme, Some congruences involving the  $p$ -adic gamma function and some arithmetical consequences, in:  *$p$ -adic functional analysis (Ioannina 2000)*, Lecture Notes in Pure and Applied Math. 222, Dekker, New York 2001.
11. M. E. Hoffman, The algebra of multiple harmonic series, *J. Algebra* **194** (1997), no. 2, 477–495.
12. M. E. Hoffman, Quasi-symmetric functions and mod  $p$  multiple harmonic sums, [arXiv:math/041319v2](https://arxiv.org/abs/math/041319v2)
13. M. E. Hoffman, The Hopf algebra structure of multiple harmonic sums, *Nuclear Physics B, Suppl.* **135** (2004), 215–219.
14. K. Iwasawa, Lectures on  $p$ -adic L-functions, Annals of mathematics studies, Princeton University press, 1972
15. M. Kontsevich, The  $1\frac{1}{2}$  logarithm, *Compositio Math.* **130** (2002), no. 2, 211–214.
16. E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.* **39** (1938), no. 2, 350–360.
17. R. Meštrović, On the mod  $p^7$  determination of  $\binom{2p-1}{p-1}$ , *Rocky Mountain Journal of Mathematics*, to appear. eprint: [arXiv:1108.1174](https://arxiv.org/abs/1108.1174)
18. R. Meštrović, Wolstenholme's theorem: its generalizations and extensions in the last hundred and fifty years (1862–2012), eprint: [arXiv:1111.3057v2](https://arxiv.org/abs/1111.3057v2)
19. J. Rosen, Multiple harmonic sums and  $p$ -adic L-function values, in preparation.
20. J. Rosen, Relations among multiple harmonic sums, in preparation.
21. R. Tauraso, More congruences for central binomial coefficients, *J. Number Theory* **130** 2010 2639–2649
22. E. Waring, *Meditationes Algebraicae*. Editio tertia recensita et aucta, Cambridge: J. Nicholson. 1782
23. L. Washington, Introduction to cyclotomic fields, *Graduate texts in mathematics, Springer-Verlag, New York* (1982)
24. L. Washington,  $p$ -adic L-functions and Sums of Powers, *Journal of Number Theory* **69** (1998), 50–61
25. J. Wolstenholme, On certain properties of prime numbers, *The Quarterly Journal of Pure and Applied Mathematics*, **5** (1862), 35–39.
26. D. Zagier, Values of zeta functions and their applications, *First European Congress of Mathematics, Vol II (Paris, 1992)*, Birkhäuser: Boston, 1994, pp. 497–512.
27. J. Zhao, Wolstenholme-type theorem for multiple harmonic sums, *Intl. J. Number Theory* **4** (2008), No. 1, 73–106.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, 530 CHURCH STREET, ANN ARBOR, MI 48109, USA,